

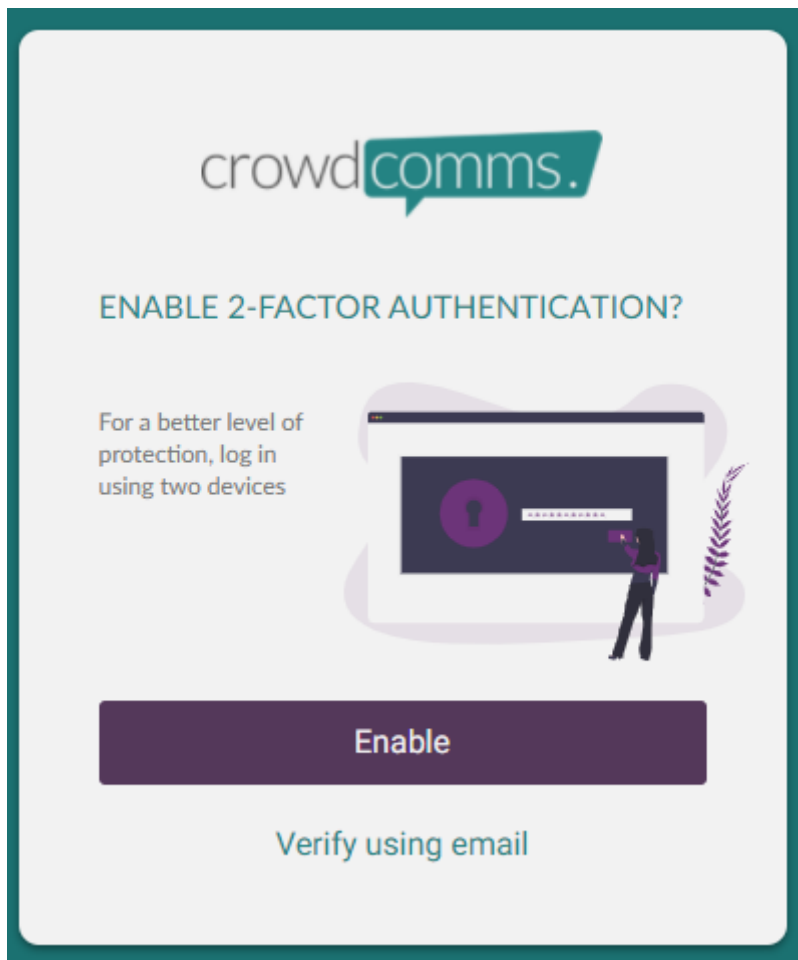
Two Factor Authentication for CMS Use

Setting Up 2FA

2FA can be enabled either by an authentication app or by getting a verification code sent to your email address.

N.B. If it is your first time accessing the CMS since the roll out of multi-factor authentication, then you may need to close your browser, re-launch and then clear your cache and cookies before accessing the CMS.

When first setting up 2FA you will be presented with this screen:



If you choose to use an authentication app then please select 'enable'. This gives better protection as it requires the use of 2 devices. If you however would rather verify by email, you can as this is still an additional layer of security.

To set up using an authentication app:

Scan the QR code or manually enter the 16 digit code (sometimes referred to as a KEY) using your Authenticator App on your personal device



Once you have either scanned the QR code or entered the 16 digit code manually, you will then be provided with a 6 digit ONE TIME ONLY code to enter

N.B The 6 digit code is only valid for 60 seconds (Your Authenticator App will provide you with a new code after this time expires).

If you are unfamiliar with authentication apps, then here are some common ones you can use:


- *Authy*
- *Microsoft Authenticator*

- *Google Authenticator*
- *LastPass*
- *OTP*

Input the 6 digit code and then click "Verify"

Two-factor Authentication

Open your third party authenticator app and enter the 6-digit code below



1

1

1

1

1

1

Back

Verify

You will now be logged into the CMS

Email Verification

If you opt for email verification, a 6 digit code will be sent to the email address associated with your CMS account.



We've sent you an access code via email. Please enter the code below to continue.

179918|

☐ Remember me on this device for 30 days



Log in

Didn't receive your code? [Resend](#)

N.B. For both routes, you have the option to 'trust this computer for 30 days' to save you verifying every time if you don't want to.

How to Manage your CMS Device

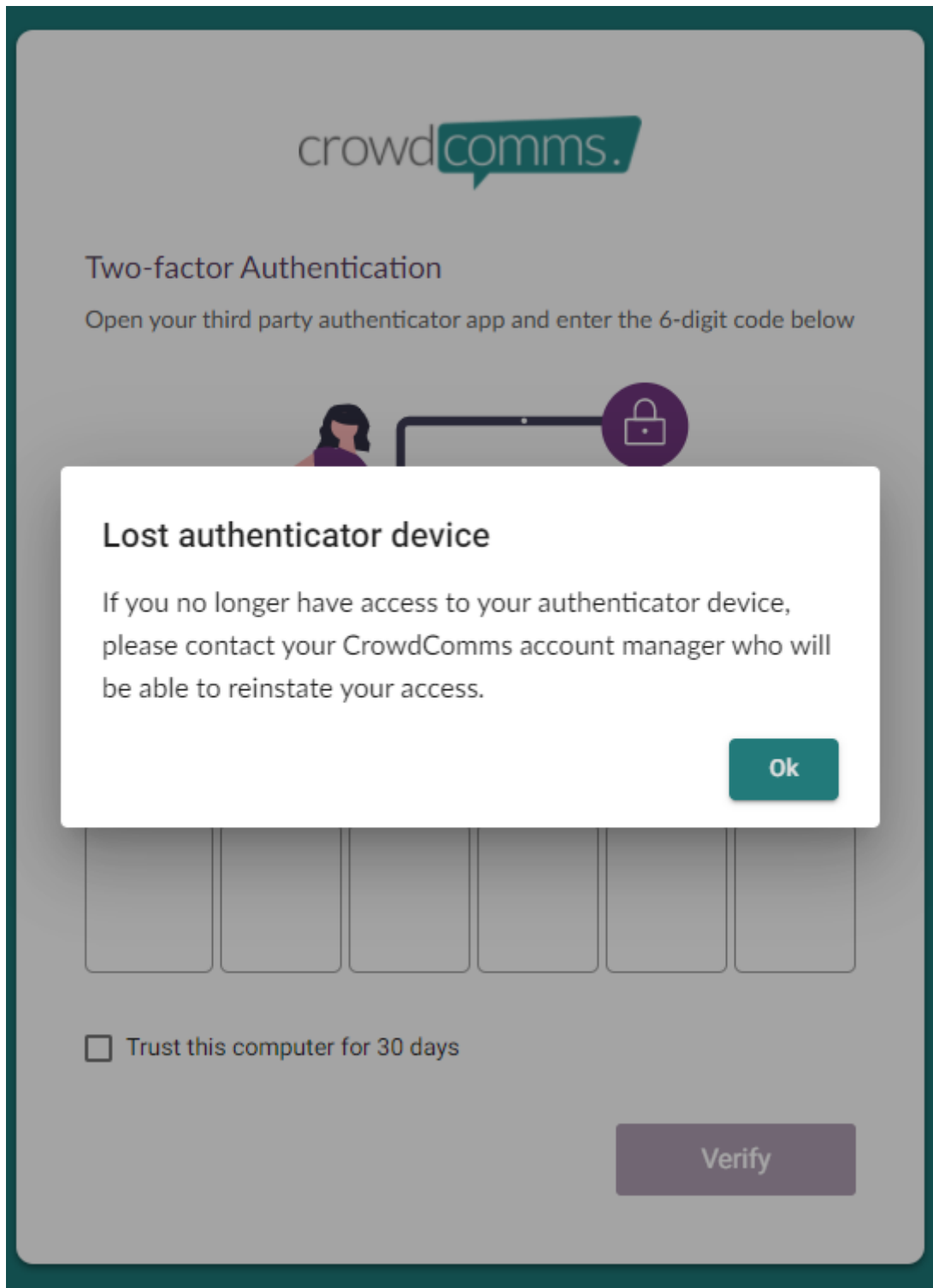
In the top-right hand profile menu you will see the option to 'manage devices'. Here you will see a device if you chose to use an authentication app. You can click the pencil to re-name it so you know exactly what device you used if helpful.

Manage your 2FA device		
Your registered device		
The device you have registered for 2-factor authentication is listed below. If you've lost access to this device, we recommend deleting it and registering a new one.		
Device name	Date added	
Device #1	Jul 8, 2021	 

N.B. You can only have one authentication device at a time for CMS access, so if you want to change devices, you will need to click the trash can to remove the first one. Once you have no devices, you will see the option to 'add device'. This will then take you through the previous

process to set up 2FA.

If you lose your device, you will need to contact your designated member of our team as only CrowdComms staff can reset this for you. You will be prompted to do this by the system anyway if you select this option when trying to login. We will then reset it for you.



The screenshot shows the CrowdComms login interface. At the top is the 'crowdcomms.' logo. Below it, the heading 'Two-factor Authentication' is followed by the instruction 'Open your third party authenticator app and enter the 6-digit code below'. A central graphic depicts a person at a computer with a padlock icon. A white modal box is overlaid in the center with the title 'Lost authenticator device' and the text: 'If you no longer have access to your authenticator device, please contact your CrowdComms account manager who will be able to reinstate your access.' An 'Ok' button is in the bottom right of the modal. Below the modal are six empty input boxes for a 6-digit code. At the bottom left is a checkbox labeled 'Trust this computer for 30 days'. At the bottom right is a 'Verify' button.

crowdcomms.

Two-factor Authentication

Open your third party authenticator app and enter the 6-digit code below

Lost authenticator device

If you no longer have access to your authenticator device, please contact your CrowdComms account manager who will be able to reinstate your access.

Ok

☐ Trust this computer for 30 days
Verify

Revision #3

Created 8 July 2021 14:16:16 by Steven Slessor

Updated 19 August 2021 16:26:36